UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

DANIEL COHEN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

BLACKBAUD, INC., a Delaware corporation, THE PRESIDENT AND FELLOWS OF HARVARD COLLEGE, a Massachusetts not-for-profit corporation, BANK STREET COLLEGE OF EDUCATION, a New York not-for-profit corporation, and LOWER EAST SIDE TENEMENT MUSEUM, a New York not-for-profit corporation,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff DANIEL COHEN ("Plaintiff") brings this Class Action Complaint against Defendants BLACKBAUD, INC. ("Blackbaud"), THE PRESIDENT AND FELLOWS OF HARVARD COLLEGE ("Harvard"), BANK STREET COLLEGE OF EDUCATION ("Bank Street"), and LOWER EAST SIDE TENEMENT MUSEUM ("Tenement Museum") (together, "Defendants") to recover damages, restitution, and injunctive relief on behalf of a Class of persons whose personal information, confidential charitable activities, and other sensitive and confidential personal information ("Private Information") was accessed without authorization by criminals as a result of Defendants' unreasonable and deficient data security practices (the "Data Breach").

Plaintiff makes these allegations on personal information as to those allegations pertaining to him, and upon information and belief, the investigation of his counsel, and facts that are a matter of public record on all other matters.

NATURE OF THE ACTION

1. Blackbaud is a cloud software and services provider for businesses, nonprofit organizations, and educational institutions.

2. Harvard, Bank Street, and the Tenement Museum (among many other institutions and businesses) hired Blackbaud for data management and data security of their customers' and donors' sensitive Private Information without sufficiently investigating and monitoring Blackbaud's data security practices.

3. Because of Defendants' unreasonable lack of oversight and lax security measures, sometime prior to May 2020, hackers accessed Plaintiff's and the other Class members' confidential Private Information without authorization, extracted and downloaded the information, and stored and maintained the information in unsecured, vulnerable, and untraceable locations for extended periods of time.

4. Blackbaud later informed its direct clients, such as Harvard, Bank Street, and the Tenement Museum (among many others) that the stolen Private Information of Plaintiff and the other Class members was destroyed, although Defendants have not explained why they rely on the word of the hackers in making that statement, while simultaneously urging Plaintiff and the other Class members to be "vigilant and promptly report any suspicious activity or suspected identity theft to [them] and to proper law enforcement authorities."

5. The Data Breach occurred sometime between February and May 2020.

6. Blackbaud did not immediately notify its clients until July 2020 and never directly informed Plaintiff and the other Class members.

7. Defendants unreasonably and wrongfully delayed in providing notification and did not even to begin to inform those affected until around August 2020.

8. Defendants failed to properly monitor the computer network and systems that housed the Private Information; failed to implement appropriate policies; and failed to properly train employees regarding cyberattacks. Had Defendants properly monitored their networks, security, and communications, they would have prevented the Data Breach or would have discovered it sooner.

9. As a direct and foreseeable result of the Data Breach, Defendants' inadequate security measures, and Defendants' unjustified delay in notification, Plaintiff and the other Class members have incurred injury in fact and sustained actual damages from the exposure and misuse of their Private Information, and reasonable attempts to safeguard their Private Information, mitigate their risk to identity theft and fraud, and remedy the effects of the Data Breach.

10. Plaintiff and the other Class members' Private Information is now at risk because of Defendants' negligent conduct and unfair acts and practices. The Private Information that Defendants collected and maintained has been placed in the hands of criminal hackers. Defendants cannot reasonably maintain that the hackers destroyed the Private Information.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security and annual audits to ensure compliance with commercially reasonable standards.

12. Plaintiff brings this action against Defendants seeking redress for their unlawful conduct and asserting claims for negligence, breach of contract, and violation of state consumer protection and data breach statutes.

PARTIES

13. Plaintiff Daniel Cohen is a natural person and is a citizen of Washington.

14. Defendant Blackbaud is a corporation existing under the laws of the State of Delaware with its principal place of business in South Carolina.

15. Defendant Harvard is a Massachusetts not-for-profit corporation with its principal place of business in Massachusetts.

16. Defendant Bank Street is a New York not-for-profit corporation with its principal place of business in New York.

17. Defendant Tenement Museum is a not-for-profit corporation established under the laws of the State of New York and chartered by the Board of Regents of the State of New York, with its principal place of business in New York.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because at least one member of the Class, as defined below is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

19. The Court has personal jurisdiction over Defendants because Defendants' negligent acts or omissions and violations of consumer protection statutes regarding the security of Plaintiff's Private Information alleged herein caused injury to Plaintiff who is located in the Western District of Washington.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the injury in this case substantially occurred in this District.

COMMON FACTUAL ALLEGATIONS

21. Sometime between February and May 2020, hackers gained unauthorized access to Blackbaud's systems and Plaintiff's and the other Class members' Private Information collected by Defendants and other clients of Blackbaud.

22. The hackers copied the Private Information and extracted it from Blackbaud's systems. Once the Private Information was acquired by the hackers, the hackers moved the Private Information to insecure locations and systems controlled by them.

23. On information and belief, the hackers were able to make many more copies of the Private Information, and/or have or will leverage the Private Information to obtain additional financial or personal information of Plaintiff and the other Class members to commit identity theft and fraud in the future.

24. According to Blackbaud's security incident notice,[1] the Data Breach was discovered in May 2020. Blackbaud claims that the Data Breach was an attempted ransomware attack, where the hackers successfully infiltrated Blackbaud's computer environment and attempted to encrypt Blackbaud's own data to lock Blackbaud out its own systems until Blackbaud paid a ransom to the hackers.

25. Blackbaud misleadingly claims it thwarted the hackers, but the hackers were able to extract a substantial amount of personal and confidential information of Plaintiff and the other Class members, in spite of and perhaps because of Blackbaud's negligent and unreasonable security practices in response to the hackers' foreseeable actions.

26. Defendants merely repeat the claim that the hackers destroyed the stolen Private Information. Defendants have not provided verification or further details regarding the disposition of the data to confirm the veracity of the hackers' dubious claim. Nor do Defendants know whether the hackers maintained the data in a sufficiently secure manner to prevent others from acquiring the Private Information while the hackers held it.

27. On information and belief, Plaintiff's and the other Class members' Private Information was copied multiple times by unscrupulous and criminal actors, not destroyed, and the data has been or may be sold and misused at a later date. Plaintiff and the other Class members act reasonably when they make reasonable payments and expenditures to avoid and mitigate the risk that criminals retained their Private Information to misuse and commit identity-theft related crimes and fraud that pose no threat of harm to Defendants, but significant harm to Plaintiff and the other Class members.

[1] *See* blackbaud.com/securityincident (last visited Aug. 31, 2020).

28. In addition to failing to secure the data with reasonable measures and preventing the Data Breach, Defendants delayed unreasonably to fulfill their obligation to provide notice of the Data Breach to Plaintiff and the other Class members. The Data Breach occurred sometime between February and May 2020, but Plaintiff and the other Class members were not notified until around August 2020.

FACTS SPECIFIC TO PLAINTIFF

29. Plaintiff previously had been a customer, client, student, or patron of Harvard, the Tenement Museum, and Bank Street.

30. On August 4, 2020, the Tenement Museum sent Plaintiff an email notifying him of the Data Breach.

31. The Tenement Museum stated that the stolen data "may have contained demographic information including customer and donor names, physical and email addresses, telephone numbers, and giving history."

32. On August 5, 2020, Bank Street sent Plaintiff an email notifying him of the Data Breach.

33. The notice from Bank Street said that the extracted data file "may have contained constituents' contact information, demographic information, and a history of their relationship with the College." However, "Blackbaud has not yet clarified which specific pieces of information may have been impacted."

34. Bank Street acknowledged "a delay between [Blackbaud's] discovery of the breach and notifying us."

35. On August 12, 2020, Harvard sent Plaintiff an email notifying him of the data breach.

36. Harvard said that the stolen data may have included demographic data for Harvard community members with a U.S. address, such as names, addresses, employment information, and birthdates, along with philanthropic engagement data.

37. Plaintiff's Private Information is highly valuable to Plaintiff, Defendants, and identity thieves, unscrupulous actors, and criminals.

38. Plaintiff and the other Class members have a right to privacy and confidentiality in their personal identification information as well as their charitable activities. The frequency and amount of donations they give to which charities tells volumes about them that they have a right to keep confidential and out of the hands of criminals and identity thieves.

39. As a result of the Data Breach, Plaintiff and the other Class members have suffered damages, and had their Private Information misused and exposed to unreasonable risks of identity theft and fraud. As a result of the Data Breach and Defendants' unreasonable delay in providing the required notice, Plaintiff took reasonable expenditures in time and money to reduce, mitigate, and prevent identity theft, misuse, and fraud that threatens to impact his finances, credit history, and the integrity of his Private Information. The full scope of the risk and what Private Information was exposed is not presently known by Plaintiff or the other Class members.

40. As a result of the Data Breach, Plaintiff has purchased a subscription to a LifeLock identity protection product and continues to invest significant time into monitoring his financial and personal accounts for suspicious activities and fraud.

CLASS ACTION ALLEGATIONS

41. **Class Definition**: Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and a nationwide Class defined as follows:

> All persons in the United States whose Private Information was accessed in the Data Breach.

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and its current or former employees, officers and directors; (3) persons who properly

execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

42. In addition, Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and nationwide Subclasses defined as follows:

> **Harvard Class**. All persons in the United States whose Private Information provided to Harvard was accessed in the Data Breach.
>
> **Bank Street College Class**. All persons in the United States whose Private Information provided to Bank Street was accessed in the Data Breach.
>
> **Tenement Museum Class**. All persons in the United States whose Private Information provided to the Tenement Museum was accessed in the Data Breach.

The following people are excluded from the Subclasses: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and its current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Subclass; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

43. **Numerosity**: The exact number of Class members is unknown to Plaintiff, but individual joinder is impracticable. On information and belief, Defendants managed the Private Information for thousands of individuals who comprise the Class. Class members can be identified through Defendants' records.

44. **Typicality**: Plaintiff's claims are typical of the claims of other members of the Class, in that Plaintiff and the Class members sustained damages arising out of the same acts and omissions of Defendants relating to their failure to oversee, monitor, and safeguard the Private Information.

45. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiff's claims are made in a representative capacity on behalf of the other members of the Class. Plaintiff has no interests antagonistic to the interests of the other members of the Class and is subject to no unique defenses. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so.

46. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' practices challenged herein apply to and affect the Class members uniformly, and Plaintiff's challenge of those practices hinge on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

47. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendants failed to maintain reasonable security procedures;

ii. Whether Defendants timely informed Plaintiff and the Class of the Data Breach;

iii. Whether Defendants' conduct constitutes negligence;

iv. Whether Defendants' conduct constitutes breach of contract;

v. Whether Defendants' conduct violates the Washington Consumer Protection Act, § 19.86.020, and the substantially similar laws of all other states;

vi. Whether Defendants' conduct violates the Washington Data Breach Act, § 19.255.010(1), and the substantially similar laws of all other states;

vii. Whether members of the Class are entitled to damages and injunctive relief.

48. **Superiority**: This case is appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. Joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small in comparison to the burden and expense of individual prosecutions of litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties and the court systems of many states and federal districts. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

COUNT I
Negligence
(On Behalf of the Class and Subclasses Against All Defendants)

49. Plaintiff incorporates paragraphs 1–49 as if fully set forth herein.

50. Each of the Defendants owed a duty to Plaintiff and the other Class members to notify them that their Private Information had been disclosed to and accessed by unauthorized criminal hackers.

51. Each of the Defendants owed a duty to Plaintiff and the other Class members to properly vet and oversee vendors who maintain, store, and manage Plaintiff's and the other Class members' Private Information and to implement and maintain reasonable data security practices to protect the Private Information from foreseeable cyberattacks and unauthorized access.

52. Defendants breached these duties and the applicable standards of care by:

a. Failing to conduct proper and reasonable due diligence over Blackbaud and its data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Private Information;

c. Failing to maintain reasonable and appropriate oversight and audits on Blackbaud and other vendors or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Private Information;

d. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the other Class members' Private Information;

e. Failing to monitor and detect confidential and sensitive data environment(s) storing Plaintiff's and the other Class members' Private Information reasonably and appropriately in order to repel or limit the Data Breach;

f. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive

business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and the other Class members' Private Information;

g. Failing to ensure that any and all unauthorized copies of Plaintiff's and the other Class members' Private Information was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the other Class members;

h. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the other Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their Private Information, and details regarding the disposition of Plaintiff's and the other Class members' Private Information at all times during the Data Breach.

53. Defendants are both the actual and legal cause of Plaintiff's and the Class members' injuries. Had Defendants adopted and maintained reasonable data security procedures and provided timely notification of the Data Breach to those affected, including Plaintiff and the other Class members, Plaintiff and the other Class members would not have been damaged or would have been damaged to a lesser degree than they actually were.

54. Plaintiff and the other Class members have suffered damages in that their stolen information may have already been used and they are now exposed to a heightened risk that their information will be misused in the future; the stolen information caused Plaintiff and the Class to incur a loss of value in their Private Information; after learning about the Data Breach, Plaintiff and many Class members purchased identity theft protection in an attempt to minimize the risks to their Private Information; and Plaintiff and the Class are still incurring ongoing damages while trying to ascertain the full scope of the problem waiting for Defendants to complete their investigation.

COUNT II
Breach of Contract
(On Behalf of the Class and Subclasses Against All Defendants)

55. Plaintiff incorporates paragraphs 1–49 as if fully set forth herein.

56. Blackbaud promises, warrants, and represents that the personal data of constituents, supporters, patients, or students of its customers will be used in accordance with applicable customers' privacy policies.[2]

57. Harvard promises, warrants, and represents that "[a]ll personally identifiable information provided by alumni is strictly reserved for use by individual alumni and Alumni Affairs & Development (AA&D) for personal and University-related purposes only," and that personal information is shared with third parties or made publicly available only in directories, class notes, and to the "extent necessary to provide and improve web services or other communications to users." https://alumni.harvard.edu/privacy (last visited Sept. 1, 2020).

58. Bank Street promises, warrants, and represents that:

> We do not disclose any of your personal information to anyone, other than to our affiliates, except as permitted by law, and to certain service providers, such as third-party Web site hosts. We will only release information about you if you direct us to do so, if compelled to do so by law, or in connection with a legitimate request for information from a government or self-regulatory organization.
>
> https://www.bankstreet.edu/privacy-policy/ (last visited Sept. 1, 2020).

59. The Tenement Museum promises, warrants, and represents that:

> The Owner may process Personal Data relating to Users if one of the following applies:
>
> - Users have given their consent for one or more specific purposes. Note: Under some legislations the Owner may be allowed to process Personal Data until the User objects to such processing ("opt-out"), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;
> - Provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;

[2] https://www.blackbaud.com/company/privacy-policy/north-america (last visited Sept. 1, 2020).

- Processing is necessary for compliance with a legal obligation to which the Owner is subject;
- Processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Owner;
- Processing is necessary for the purposes of the legitimate interests pursued by the Owner or by a third party.

https://www.iubenda.com/privacy-policy/7973183/legal (last visited Sept. 1, 2020).

60. In addition, the Tenement Museum promises, warrants, and represents that "Users have the right, under certain circumstances, to restrict the processing of their Data. In this case, the Owner will not process their Data for any purpose other than storing it." *Id.*

61. In addition, the Tenement Museum promises, warrants, and represents that "Users are also entitled to learn about the legal basis of Data transfers to a country outside the European Union or to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Owner to safeguard their Data." *Id*.

62. The terms of Harvard, Bank Street, and the Tenement Museum's privacy policies are incorporated into the terms governing the relationship between Blackbaud and Plaintiff and the other Class members.

63. Defendants breached the foregoing contractual terms resulting in the Data Breach, in one or more of the following ways:

a. Failing to conduct proper and reasonable due diligence over Blackbaud and its data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Private Information;

c. Failing to maintain reasonable and appropriate oversight and audits on Blackbaud and other vendors or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and the other Class members' Private Information;

d. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and the other Class members' Private Information;

e. Failing to monitor and detect its confidential and sensitive data environment(s) storing Plaintiffs' and the other Class members' Private Information reasonably and appropriately in order to repel or limit the Data Breach;

f. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and the other Class members' Private Information;

g. Failing to ensure that any and all unauthorized copies of Plaintiff's and the other Class members' Private Information was deleted, destroyed, rendered unable to be used, or returned to Plaintiff and the other Class members;

h. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and the other Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their Private Information, and details regarding the disposition of Plaintiff's and the other Class members' Private Information at all times during the Data Breach.

64. As a proximate result of Defendants' breaches of contract described above and the resulting injuries to Plaintiff and the other Class members, as herein alleged, Plaintiff and the other Class members have incurred damages.

65. Plaintiff and the other Class members have suffered damages in that their stolen information may have already been used and they are now exposed to a heightened risk that their information will be misused in the future; the stolen information caused Plaintiff and the Class to incur a loss of value in their Private Information; after learning about the Data Breach, Plaintiff and many Class members purchased identity theft protection in an attempt to minimize the risks to their Private Information; and Plaintiff and the Class are still incurring ongoing damages while trying to ascertain the full scope of the problem waiting for Defendants to complete their investigation.

COUNT III
Violation of the Washington Consumer Protection Act, RCW § 19.86.010, *et seq.*, and Substantially Similar Laws of Other States
(On Behalf of the Class and Subclasses Against All Defendants)

66. Plaintiff incorporates paragraphs 1–49 as if fully set forth herein.

67. RCW § 19.86.020 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

68. Defendants engaged in unfair acts or practices by failing to establish appropriate oversight and monitoring of the data security practices for the systems storing and processing Plaintiff's and the other Class members' Private Information, failing to implement and maintain reasonable data security practices for the systems storing and processing the systems, failing to prevent the systems from being accessed without authorization by foreseeable attacks by hackers on such information, failing to respond to the Data Breach properly and adequately to prevent the hackers from acquiring Plaintiff's and the other Class members' Private Information, and failing to timely notify Plaintiff and the other Class members of the Data Breach when there was not justifiable reason to keep the Data Breach secret.

69. Defendants' conduct occurred in commerce.

70. Defendants' conduct impacts the public interest by allowing many consumers' personal identifying information to be disclosed to unauthorized third parties with criminal intent.

71. As a proximate result of Defendants' unfair acts and practices described above and the resulting injuries to Plaintiff and the other Class members, as herein alleged, Plaintiff and the other Class members have incurred damages.

72. Plaintiff and the other Class members have suffered damages in that their stolen information may have already been used and they are now exposed to a heightened risk that their information will be misused in the future; the stolen information caused Plaintiff and the Class to incur a loss of value in their Private Information; after learning about the Data Breach, Plaintiff and many Class members purchased identity theft protection in an attempt to minimize the risks to their Private Information; and Plaintiff and the Class are still incurring ongoing damages while trying to ascertain the full scope of the problem waiting for Defendants to complete their investigation.

73. As a result, Plaintiff and the other Class members are entitled to actual damages, costs, and attorney's fees pursuant to RCW § 19.86.090.

74. Plaintiff is further requesting treble damages pursuant to RCW § 19.86.090 due to the reprehensible nature of Defendants' conduct, as described herein.

COUNT IV
Violation of the Washington Data Breach Act, RCW § 19.255.010, *et seq*.
and Substantially Similar Laws of Other States
(On Behalf of the Class and Subclasses Against All Defendants)

75. Plaintiff incorporates paragraphs 1–49 as if fully set forth herein.

76. Defendants owed a statutory duty to promptly disclose the Data Breach to Plaintiff and the other Class members, as specified in each state's statute.

77. Defendants failed to promptly disclose the Data Breach to Plaintiff and the other Class members, in violation of the respective disclosure deadlines in each state's statute.

78. Defendants became aware of the Data Breach at sometime between February and May 2020.

79. Blackbaud never notified Plaintiff or any Class members at any time.

80. Defendants unreasonably delayed in providing the required notification to Plaintiff and the other Class members.

81. The Tenement Museum gave notice to Plaintiff on August 4, 2020.

82. Bank Street gave notice to Plaintiff on August 5, 2020.

83. Harvard gave notice to Plaintiff on August 12, 2020.

84. Plaintiff and the other Class members have suffered damages in that their stolen information may have already been used and they are now exposed to a heightened risk that their information will be misused in the future; the stolen information caused Plaintiff and the Class to incur a loss of value in their Private Information; after learning about the Data Breach, Plaintiff and many Class members purchased identity theft protection in an attempt to minimize the risks to their Private Information; and Plaintiff and the Class are still incurring ongoing damages while trying to ascertain the full scope of the problem waiting for Defendants to complete their investigation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff DANIEL COHEN, individually and on behalf of the Class, prays for the following relief:

A. An order certifying the Class as defined above, appointing Plaintiff as the Class representative and appointing Plaintiff's counsel as Class counsel;

B. An order declaring that Defendants' actions, as set out above, violate the Washington Consumer Protection Act, § 19.86.020; and substantially similar laws of other states;

C. An order declaring that Defendants' actions, as set out above, constitute negligence;

D. An order declaring that Defendants' actions, as set out above, constitute a breach of contract;

E. An order declaring that Defendants' actions, as set out above, violate the Washington Data Breach Act, § 19.255.010, and substantially similar laws of other states;

F. An injunction requiring Defendants to maintain reasonable security measures;

G. Judgment in favor of Plaintiff and the Class and against all Defendants, jointly and severally, and award of damages, including punitive damages, attorney's fees and costs;

H. Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Dated this ___ day of September, 2020.

LAW OFFICE OF CARL J. MARQUARDT PLLC

/s/ *Carl J. Marquardt*
Carl J. Marquardt (WA Bar No. 23257)
1126 34th Avenue, Suite 311
Seattle, WA 98122
Tel: (206) 388-4498
Email: carl@cjmlawoffice.com

Mark L. Javitch (pro hac vice pending)
JAVITCH LAW OFFICE
480 S. Ellsworth Avenue
San Mateo CA 94401
Tel: (650) 781-8000
Fax: (650) 648-0705

Thomas A. Zimmerman, Jr. (pro hac vice pending)
tom@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Tel: (312) 440-0020
Fax: (312) 440-4180
www.attorneyzim.com

Attorneys for Plaintiff and the Putative Class